REMARKS

The Office Action mailed on April 12, 2006 has been received and reviewed. Claims 1-30 are in the case. Claims 1-3, 5-6, 13-16, 18-19, 20-23, and 25-29 were rejected under 35 U.S.C. 102(b) as being anticipated by Hardjono (6,425,004). Claims 7-9 and 11-12 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (6,425,004) in view of *Microsoft Computer Dictionary* (Microsoft). Claims 4, 17, 24, 30 were rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (6,425,004) in view of Goldberg et al. (US2003/0115516). Claim 10 was rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (6,425,004) in view of *Microsoft Computer Dictionary* (Microsoft) in further view of Goldberg et al. (US2003/0115516).

Applicants would like to remind the Examiner of the meaning of the word inherent. The dictionary web site www.dictionary.com returns the following definition for inherent:

> in·her·ent ɪnˈhɪərənt, -ˈhɛr- - Show Spelled Pronunciation[in-**heer**-*uh* nt, -**her**-]
> Pronunciation Key - Show IPA Pronunciation
>
> *-adjective*
>
> 1. existing in someone or something as a permanent and inseparable element, quality, or attribute.

Applicants agree with the preceding definition. The present invention teaches the use of an inherent identifier to directly determine which communication module is faulty in a network of communicating devices. Applicants assert that using an inherent identifier offers advantages over non-inherent identifiers and that the prior art does not teach such a use.

Regarding the rejection of claims 1-3, 5-6, 13-16, 18-19, 20-23, and 25-29 under 35 U.S.C. 102(b) as being anticipated by Hardjono (6,425,004) and claims 7-9 and 11-12 under 35U.S.C. 103(a) as being unpatentable over Hardjono in view of *Microsoft Computer Dictionary*. Applicants assert that Hardjono does not disclose nor enable utilizing an inherent identifier associated with a

device as a unique identifier for a device. Rather Hardjono teaches the use of non-inherent device and sector keys provided by a domain server. Consequently, practicing Hardjono requires that a domain server be present on the network and functioning properly in order to assign identifiers to devices.

Furthermore, Hardjono is directed to authentication of packets rather than identification of a faulty communication module. Specifically, the method of Hardjono uses a sector key and sector tag to determine whether to accept or drop a packet. Accepting or dropping a packet differs from determining which communication module is faulty.

Regarding, the assertion that Hardjono teaches identifying the faulty device using a router tag in column 6 lines 34-38 or elsewhere. Applicants respectfully disagree and encourage the Examiner to read the remainder of the paragraph where Hardjono discusses his trial and error approach for identifying which router is misbehaving:

> When the STA in the originating sector receives the packet (either from the STA in the receiving sector, if the receiving sector is different than the originating sector, or from the receiving router, if the receiving sector is the same as the originating sector), the STA tries to identify the misbehaving router. Because the receiving router authenticated that the packet originated in the originating sector, it is probable that the packet did originate within the originating sector and that the misbehaving router is therefore within the originating sector. However, it is possible that the misbehaving router is actually in another sector and is sending invalid information that appears to be sector-authentic. This could happen, for example, if the misbehaving router has been compromised by an intruder or "hacker," or if there is a misconfiguration within the router network.
>
> Therefore, the STA attempts to authenticate the packet by verifying the router tag **404** in the packet. Specifically, the STA uses the router keys for the routers within the STA's sector to determine whether one of the routers within the STA's sector is the originating router. In order to determine whether a particular router is the originating router, the STA determines the router key for the router, and computes a router verification tag for the packet based upon the data field **200**, the sector tag **306**, and the router key. The STA then compares the router verification tag to the router tag **404** in the packet. If the router verification tag matches the router tag **404**, then the STA has successfully identified the originating router. However, if the router verification tag does not match the router tag **404**, then the STA repeats the same process for another router within the STA's sector. If none of the routers within the STA's sector is authenticated as the originating router, then the STA may forward the packet to other STAs, which in turn perform the same set of steps to determine whether any of the routers in their respective sectors is the originating router for the packet. The STAs may also notify a network administrator that there is an unidentified misbehaving router.

Notice that Hardjono teaches repeated testing of a verification tag against a router tag until a match is found. Notice also that Hardjono discloses that "The STAs may also notify a network administrator that there is an **unidentified** misbehaving router." Applicants assert that such a trial and error process does not read on the claim limitations presented by the Applicants. However, in order to prevent a misinterpretation of Applicants' claims, Applicants have amended the independent claims to further clarify the differences of the present invention with the prior art. Specifically, Applicants have amended the last clause of claim 1 to read: "the validation module further configured to directly identify ~~the communication module as faulty~~which communication module is faulty via the inherent identifier if the second check value is valid and the first check value is not valid." Similar amendments where made to the other independent claims.

CONCLUSION

In summary, while the use of CRC and LRC data verifications are well known in the prior art, the ability to determine a data error and immediately identify which intermediate device is faulty is a novel aspect of the present invention. Additionally, the use of an identifier that is inherently specific to the device such as a "hardware address or an abstraction of the hardware address" (Benhase, paragraph 0060) allows the faulty device to be directly identified without requiring the use of a domain controller or the like. Applicants again reiterate that neither of these teachings are disclosed or anticipated in the cited prior art. Applicants therefore assert that the combination of elements cited in Applicants' claims is novel and non-obvious.

For the reasons stated above, Applicants assert that claims 1-30 are in condition for allowance and respectfully request prompt allowance of the pending claims. In the event that the Examiner finds any remaining impediments to the prompt allowance of any of these claims which could be clarified in a telephone conference, the Examiner is respectfully urged to initiate the same with the undersigned.

Respectfully submitted,

Date: February 27, 2007

/Brian C. Kunzler/

Kunzler & Associates
8 E. Broadway, Suite 600
Salt Lake City, Utah 84111
Telephone: 801/994-4646

Brian C. Kunzler
Reg. No. 38,527
Attorney for Applicant